UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/780,848	02/18/2004	Michael Thomas Kurdziel	RF-235 (50589)	2513

7590 10/24/2007

CHRISTOPHER F. REGAN, ESQUIRE
ALLEN, DYER, DOPPELT, MILBRATH & GILCHRIST, P.A.
P.O. Box 3791
Orlando, FL 32802-3791

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
10/24/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/780,848	KURDZIEL ET AL.	
	Examiner	Art Unit	
	Abdulhakim Nobahar	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 August 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to applicants' amendment filed on 08/03/2007.

2. Claims 1-26 are pending.

3. Applicant's arguments with respect to the rejections of claims 1-26 under 35 USC § 102 have been fully considered and are persuasive. Therefore, the rejections have been withdrawn. However, upon further consideration of the amended claims, a new ground(s) of rejection is made.

4. When responding to the Office action, Applicant is advised to clearly point out the patentable novelty the claims present in view of the state of the art disclosed by the reference(s) cited or the objection made. A showing of how the amendments avoid such references or objections must also be present. See 37 C.F.R. 1.111(c).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-26 are rejected under 35 U.S.C. 102(b) as being anticipated by the Luyster (2002/0118827 A1).

In reference to claims 1, 10 and 18, Luyster discloses:

a cryptographic device (see Figs. 3, 9 and 13) comprising:

a key scheduler providing a key data block comprising a plurality of sub-key data blocks (see paragraph 0043, 0086, 0096 and 0245); and

An input stage receiving an input data block (see paragraph 0102 and Fig. 3, box 50) and a key data block comprising a plurality of sub-key data blocks (see paragraph 0112, Fig. 4 and paragraphs 0235 and 0247), and generating a plurality of first signals therefrom, where the sub key data blocks are the subkeys generated for use in the AES protocol (see paragraph 0251).

An intermediate stage connected to said input stage (see paragraphs 0011 and 0157) and comprising

A plurality of substitution units, each substituting data within a respective first signal (see paragraphs 0015, 0022, 0100, 0134 and 0153, where S-boxes corresponds to the recited substitution units), and

A diffuser connected to said plurality of substitution units for mixing data to generate a diffused signal (see paragraphs 0087 0109 and 0218),

An output stage connected to said intermediate stage for repetitively looping back the diffused signal to said input stage for combination with a next sub-key data block (see paragraphs 0008-0012, 0088, 0099 and 0131; Figs. 3 and 4, where rounds correspond to the recited repetitively looping back),

In reference to claims 2 and 19, Luyster discloses:

a cryptographic device according to claim 1 wherein the looping back is repeated a predetermined number of times; and wherein said output stage provides an output

signal for the cryptographic device after the repetitively looping back is complete (see paragraphs 0053, 0102 and 0155).

In reference to claims 3, 11 and 20, Luyster discloses:

a cryptographic device according to claim 2 wherein the output signal is further combined with a final sub-key data block (see Fig. 3, box 82).

In reference to claims 4, 12 and 21, Luyster discloses:

a cryptographic device according to Claim 1 wherein each substitution unit performs a non-linear substitution based upon at least one look-up table (see paragraphs 0102 and 0111).

In reference to claims 5, 13 and 22, Luyster discloses:

a cryptographic device according to claim 1, wherein said diffuser comprises a shift register and a loop-up table associated therewith (see paragraphs 0149, 0195, 0213 and 0323).

In reference to claims 6, 14 and 23, Luyster discloses:

a cryptographic device according to claim 1 wherein said diffuser comprises a plurality of shift registers and a plurality of look-up tables associated therewith (see paragraphs 0195, 0323 and 0340).

In reference to claims 7, 15 and 24, Luyster discloses:

a cryptographic device according to claim 1 wherein said output stage performs a row-shift operation on the diffused output signal before being looped back to said input stage (see paragraph 0195, where circular bit rotation corresponds to the recited row-shift operation).

In reference to claims 8, 16 and 25, Luyster discloses:

a cryptographic device according to claim 1 wherein said output stage performs a column-mix operation on the diffused output signal being looped back to said input stage (see paragraphs 0190, 0195 and 0207).

In reference to claims 9, 17 and 26, Luyster discloses:

A cryptographic device according to Claim 1 wherein said output stage comprises a counter for counting a number of times the diffused output signal is looped back to said input stage (see paragraphs 0053, 0102 and 0155, where a constant or pre-selected number of rounds indicate the use of a counter to count the number of rounds being completed).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US Patent No. 6,769,063 B1 to Kanda et al.

US Patent No. 6,189,095 B1 to Coppersmith et al.

US Patent No. 6,0289,39 A to Yin.

US Patent No. 7,254,231 B1 to Van Dyke et al.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 571-272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Abdulhakim Nobahar
Examiner
Art Unit 2132 A. N.

October 17, 2007

Benjamin E. Lanier
Examiner AU 2132